July 2020

Our School Christian Vision

With thankfulness, courage and love, we strive to improve heart and mind.

At Chilton Foliat Primary School we honour our educational heritage, supported by a strong Christian ethos. We strive to provide a diverse education that inspires children to develop a **thirst for knowledge**. This is delivered in a safe, supportive and nurturing environment promoting self-discipline, motivation and excellence in learning. We encourage strong partnerships and positive relationships amongst pupils, parents, carers, staff and the wider community.

Data Protection Policy

CONTENTS

1. AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the **General Data Protection Regulation (GDPR)** and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the **Data Protection Bill.**

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the **GDPR** and the ICO's **code of practice for subject access requests.** It also reflects the ICO's **code of practice** for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the **Education (Pupil Information) (England) Regulations 2005**, which gives parents the right of access to their child's educational record.

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental

	• Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 GOVERNING BOARD

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 DATA PROTECTION OFFICER

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their SLA.

Our DPO is SchoolPro TLC Limited and is contactable via GDPR@SchoolPro.uk

5.3 HEADTEACHER
The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 ALL STAFF
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. DATA PROTECTION PRINCIPLES
The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. COLLECTING PERSONAL DATA

7.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY
We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school, as a public authority, can perform a **public task,** and carry out its official functions
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- Where the above does not apply we shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil)

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, we intend to rely on Public Task as a basis for processing, where this is not appropriate, we will get parental consent for processing (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we may seek consent if necessary, before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO / Headteacher.

9.2 CHILDREN AND SUBJECT ACCESS REQUESTS

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is the basis for processing
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Headteacher or DPO. If staff receive such a request, they must immediately forward it to the DPO or Headteacher.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, or those with parental responsibility, have a legal right to free access to their child's educational records.

11. BIOMETRIC RECOGNITION SYSTEMS

The school does not collect or otherwise process biometric data at this point in time.

12. CCTV

The school does deploy CCTV on premise at this point in time.

13. PHOTOGRAPHS AND VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.

We will not seek consent from parents/carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and school displays. We will process these images under the legal basis of Public Task.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on public area notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not usually accompany them with any other personal information about the child, to ensure they cannot be identified.

See our E-Safety policy for more information on our use of photographs and videos.

14. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must follow the relevant school procedures and ensure all records and copies are returned to the school
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety policy doc on school website on acceptable practice to delete where appropriate])
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. TRAINING

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. MONITORING ARRANGEMENTS

This policy will be reviewed and updated **every 2 years** and shared with the full governing board.

20. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Freedom of information publication scheme on our school website.

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on **guidance on personal data breaches** produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Headteacher.
- The Headteacher will investigate the report, and determine whether a breach has occurred. To decide, the Headteacher will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The headteacher will seek advice from the DPO and alert the chair of governors
- The Headteacher will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the DPO and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen based on the Headteacher investigation to advise the Headteacher further
- The DPO in conjunction with the Headteacher, will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO will notify the ICO.

- The Headteacher will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Breach-Log document in electronic format.
- Where the ICO must be notified, the DPO or Headteacher will do this via the 'report a breach' page of the ICO website. As required, the report will set out:
    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the School will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the they expect to have further information. The Headteacher or DPO will submit the remaining information as soon as possible
- The School will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the School will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The School will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The School will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored are in the Breach-Log document in electronic format.

- The DPO and headteacher will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

APPENDIX 2: OTHER IMPORTANT INFORMATION

THIS POLICY SHOULD BE READ AND UNDERSTOOD IN CONJUNCTION WITH THE FOLLOWING POLICIES AND GUIDANCE:

- The Data Protection Act 1998
- Becta: Information Risk Management and Protective Marking
- Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
- Records Management Society – Tool Kit for Schools

PRINCIPLES:

Colleagues within schools have increasing access to a wide range of sensitive information[1]. There are generally two types of sensitive information; personal data concerning the staff and pupils and commercially sensitive financial data. It is important to ensure that both types of information are managed in a secure way at all times.

Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the Data Protection Act as ***"Data relating to a living individual who can be identified from the data".*** The Act gives 8 principles to bear in mind when dealing with such information. Data must:

1. be processed fairly and lawfully, be collected for a specified purpose and not used for anything incompatible with that purpose
2. be adequate, relevant and not excessive
3. be accurate and up-to-date
4. not be kept longer than necessary
5. be processed in accordance with the rights of the data subject
6. be kept securely, not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

The Data Protection Act states that some types of personal information demand an even higher level of protection, this includes information relating to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership

[1] The terms, "Information" and "data" are treated as the same for the purposes of this policy.

- physical or mental health or condition
- sexual life (orientation)
- the commission or alleged commission by them for any offence or any proceedings for such, or the sentence of any court in such proceedings.

The three questions below can be used to quickly assess whether information needs to treated securely, i.e.

1. Would disclosure / loss place anyone at risk?
2. Would disclosure / loss cause embarrassment to an individual or the school?
3. Would disclosure / loss have legal or financial implications?

If the answer to any of the above is “yes” then it will contain personal or commercially sensitive information and needs a level of protection. (A more detailed assessment guide is contained in Appendix 4 of this document.

PROCEDURES AND PRACTICE:

The following practices will be applied within the school:

- The amount of data held by the school should be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personal data held by the school will be securely stored and sent by secure means.

AUDITING:

The school will be aware of **all** the sensitive data it holds, be it electronic or paper.

- A register (Appendix B) will be kept detailing the types of sensitive data held, where and by whom, and will be added to as and when new data is generated.
- How long these documents need to be kept will be assessed using the Records Management Toolkit.
- Audits will occur in lie with the timetable detailed in Appendix 5 of this document.

This register will be sent to all staff each year to allow colleagues to revise the list of types of data that they hold and manage.

The audit will be completed by a member of staff responsible for data protection.

RISK ASSESSMENT:

If it has not already been undertaken, the school will carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available.

Carrying out a risk assessment will generally involve:

- How sensitive is the data?
- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?
- Does anything further need to be done to reduce the likelihood?

Once the risk assessment has been completed, the school can decide how to reduce any risks or whether they are at an acceptable level.

Risk assessment will be an on-going process and the school will have to carry out assessments at regular intervals as risks change over time.

SECURING AND HANDLING DATA HELD BY THE SCHOOL:

The school will encrypt[2] any data that is determined to be personal or commercially sensitive in nature. This includes fixed computers, laptops and memory sticks.

Staff should **not** remove or copy sensitive data from the organisation or authorised premises unless the media is:

- encrypted,
- is transported securely
- will be stored in a secure location.

[2] Encryption of computers and memory sticks can be provided by the school's technical support. Guidance is available from http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

This type of data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc).

Data transfer should be through secure websites e.g. S2S, SecureNet Plus, common transfer files and school census data. If this is not available then the file must be minimally password protected or preferably encrypted[3] before sending via email, the password must be sent by other means and on no account included in the same email. A record of the email should be kept, to identify when and to whom the email was sent, (e.g. by copying and pasting the email into a Word document).

Data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. safe / fire safe / remote backup.

All staff computers will be used in accordance with the Teacher Laptop Policy (Appendix C)

When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by a technician using a recognised tool, e.g. McAfee Shredder.

The school's wireless network (WiFi) will be secure at all times[4].

The school will identify which members of staff are responsible for data protection. The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc. know what data is held, who has access to it, how it is retained and disposed of. Appendix B details which members of staff are responsible for which data. This is shared with all staff concerned within the school.

Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. **This information must not be stored on a personal (home) computer.**

Members of staff (e.g. senior administrators) who are given full, unrestricted access to an organisation's management information system should do so over an encrypted connection and use two-factor authentication, which is available to SIMS users from Capita. **This information must not be stored on a personal (home) computer.**

[3] The ICES bulletin has a useful guide explaining how WINZIP a free application can be used to encrypt files that need to be sent either through S2S, SecureNet or email: http://www.teachernet.gov.uk/_doc/14782/ICES%20Bulletin%20-%20issue%2041%20v1-0Final.pdf

[4] The school will use WPA2 (or WPA if WPA2 is not available). The older standard WEP will not be used.

The school will keep necessary pupil and staff information in accordance with the Records Management Society's guidance (see references at the end of this document).

The school should securely delete commercially sensitive or personal data when it is no longer required as per the Records Management Society's guidance.

All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them, this will be the responsibility of the Head Teacher.

When sensitive data is to be sent out of the school it must be done in a secure way. The Information About Children Education and schools (ICES) March Bulletin (no 41) contains a number of useful guidance sections and appendices that cover the issues of Information Sharing and details of how to securely transfer data between schools, LA and Government departments[5].

[5] http://www.teachernet.gov.uk/_doc/14782/ICES%20Bulletin%20-%20issue%2041%20v1-0Final.pdf

APPENDIX 3:
HELP SHEET FOR ASSESSING RISK OF SHARING INFORMATION

In deciding the most appropriate way to share information and the level of security required, you must always take into consideration the nature of the information and the urgency of the situation, i.e. take a risk based approach to determining appropriate measures.

The simplified process described below will help organisations to choose the appropriate level of security to consider when emailing information.

Step 1
Imagine a potential security breach (e.g. a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

1. Will it affect or identify any member of the school or community?
2. Will someone lose / be out of pocket by / more than £100?
3. Will it cause any kind of criminal case to fail?
4. Is there a risk of discomfort / slur upon professional character of someone?
5. Is anyone's personal safety at risk?
6. Will it embarrass anyone?

If you answered **NO** to all the questions, the document does not contain sensitive information. If you answered yes to any of the questions, the document with include some sensitive information and therefore requires a level of protection.

Step 2
Imagine the same potential security breach as above, and consider:

7. Will it affect many members of the school or local community and need resources locally to manage it?
8. Will an individual or someone who does business with the school lose / be out of pocket by £1,000 to £10,000?
9. Will a serious criminal case or prosecution fail?
10. Is someone's personal safety at a moderate risk?
11. Will someone lose his or her professional reputation?
12. Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If you have answered **yes** to any of the above questions the document contains sensitive information and additional security should be considered, such as, password protecting the document before

you email it to a colleague outside of your organisation. Further information about how to achieve this can be found on the ICES bulletin (number 41)[6].

However, if you think that the potential impact exceeds that stated in the question (for example, someone's personal safety is at high risk) think very carefully before you release this information.

Step 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection / security; organisations should err on the side of caution.

[6] http://www.teachernet.gov.uk/_doc/14782/ICES%20Bulletin%20-%20issue%2041%20v1-0Final.pdf

APPENDIX 4:
REGISTER OF SENSITIVE DATA HELD BY THE SCHOOL

Type of data	Held on	Period to be retained	Type of protection	Who can access the data
Pupil SEN data	SENCO laptop		Data is encrypted on laptop	SENCO and Headteacher

Activity	Frequency	Lead
Audit of data held	Annually	Head and admin officer
Encrypting sensitive data	On-going	All staff
Reviewing data backup procedures	Annual	Head and ICT Technician
Identifying staff responsible for data security and keep log of names and roles.	Annual	Head
Wiping of laptop data when re-issued	Annual and then when necessary.	ICT Technician
Wiping of laptop data when discarded	As necessary	ICT Technician

APPENDIX 5:

TIMETABLE FOR INFORMATION SECURITY MANAGEMENT

This policy is reviewed every two years or as necessary

Staff Computer Use Policy

Chilton Foliat C of E VA primary school

Date:

- Passwords that I use to access school systems will be kept secure and secret – if I have reason to believe that my password is no longer secure I will change it.

- I acknowledge that the computer provided for me to use remains the property of the school and should only be used for school business.

- I will not access the files of others or attempt to alter the computer settings.

- I will not update web content or use pictures or text that can identify the school, without the permission of the Headteacher.

- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school. I will seek permission with the school's technician / Network Manager should I need to install additional software.

- I will always adhere to the copyright.

- I will always log off the system when I have finished working.

- I understand that the school may, in line with Oakford Internet, monitor the Internet sites I visit.

- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager / school technician / headteacher.

- Any e-mail messages I send will not damage the reputation of the school.

- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be forwarded.

- I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material[7].

- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.

- I understand that I am responsible for the safety of school data that I use or access.

- In order to maintain the security of data I will take the following steps:

    - I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.

    - I will not save data files to a PC or laptop other than that provided by the school.

    - If I need to transfer sensitive data files and no secure electronic option is available I will only do so using the encrypted USB key provided by the school.

    - Sensitive data will only be sent electronically through a secure method, e.g. SecureNet Plus. If this is not available then the minimum requirement is to password protect the document before attaching it to email.

Sensitive data includes:

Pupil reports

SEN records

[7] Legislative guidance is available from the Internet Watch Foundation: http://www.iwf.org.uk/police/page.22.htm

Letters to parents

Class based assessments

Exam results

Whole school data

Medical information

Information relating to staff, e.g. Performance Management reviews.

If I am in any doubt as to the sensitivity of data I am using, I will consider these questions:

- Would disclosure / loss place anyone at risk?
- Would disclosure / loss cause embarrassment to an individual or the school?
- Would disclosure / loss have legal or financial implications?

If the answer to any of these questions is yes, then the data should be treated as sensitive.

I understand that if I do not adhere to these rules outlined in this policy, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow including notification to professional bodies where a professional is required to register. If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may be reference for investigation by the Police and could recorded on any future Criminal Record Bureau checks.

Name…….

Date……..

References:

The Data Protection Act 1998:

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Becta: Data handling security guidance for schools http://schools.becta.org.uk/index.php?catcode=ss_lv_saf_dp_03&rid=14734&section=lv

Information Commissioner's Office

www.ico.gov.uk

Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008

http://publications.everychildmatters.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-00807-2008&

Records Management Society – Tool Kit for Schools:

http://www.rms-gb.org.uk/resources/848